CUSTOMER NO. 24498
SERIAL NO. 10/517,134

RECEIVED
CENTRAL FAX CENTER
APR 08 2008

PU020267

Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of the Claims

1. (original) In a wireless local area network having an interworking function, a method for interworking between the wireless local area network and a second network, the wireless local area network and the second network capable of communicating with a broker, the method comprising the steps of:

receiving from the broker, a first key;

receiving from a user device, a second network to user certificate that includes a broker to second network certificate and a second key;

authenticating the broker to second network certificate using the first key to derive a third key;

authenticating the second network to user certificate using the third key to derive the second key;

generating a session key, encrypting the session key using the second key, and transmitting the encrypted session key to the user device; and

communicating with the user device using the session key.

2. (original) The method of claim 1, wherein the second network to user certificate further includes a user subscription level that indicates whether a user has a subscription for an interworking service, and the generating step is performed in response to the user subscription level.

3. (original) The method of claim 1, wherein the second network to user certificate further includes an expiration time of the second network to user certificate, and the method further comprises the step of checking the expiration time to determine

PAGE 2/9 * RCVD AT 4/8/2008 8:20:38 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:609 734 6888 * DURATION (mm-ss):01-46

RECEIVED
CENTRAL FAX CENTER
APR 08 2008

whether the second network to user certificate has expired.

4. (original) The method of claim 1, further including the step of generating a wireless local area network to user certificate that is signed with a fifth key and includes the session key, whereby the wireless local area network is able to be authenticated.

5. (original) In a wireless local area network having an interworking function, a method for interworking between the wireless local area network and a second network, the wireless local area network and the second network capable of communicating with a broker, the method comprising the steps of:

receiving, from the broker, a broker public key;

receiving, from a user device, a second network to user certificate, which is signed with a second network private key and includes a broker to second network certificate and a user public key, the broker to second network certificate being signed with a broker private key and including a second network public key;

authenticating the broker to second network certificate using the broker public key and deriving the second network public key;

authenticating the second network to user certificate using the second network public key and deriving the user public key;

generating a session key, encrypting the session key using the user public key, and transmitting the encrypted session key to the user device; and

communicating with the user device using the session key.

6. (original) The method of claim 5, wherein the second network to user certificate further includes a user subscription level that indicates whether a user has a subscription for an interworking service, and the generating step is performed in response to the user subscription level.

7. (original) The method of claim 5, wherein the second network to user certificate further includes an expiration time of the second network to user certificate,

PAGE 3/9 * RCVD AT 4/8/2008 8:20:38 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:609 734 6888 * DURATION (mm-ss):01-46

and the method further comprises the step of checking the expiration time to determine whether the second network to user certificate has expired.

8. (original) The method of claim 5, further including the step of providing the user device with an ability to authenticate the wireless local area network.

9. (original) The method of claim 8, wherein the providing step comprises the steps of:

receiving a broker to wireless local area network certificate signed with the broker private key and includes a wireless local area network private key;

generating a wireless local area network to user certificate that is signed with the wireless local area network private key and includes the encrypted session key; and

transmitting the wireless local area network to user certificate.

10. (original) A method for communicating with a wireless local area network using a user device that has a subscription to a second network, the second network having an interworking contract with the wireless local area network, the wireless local area network and the second network capable of communicating with a broker, the method comprising the steps of:

receiving, from the second network, a second network to user device certificate, which is signed with a second network private key, and includes a broker to network certificate and a user public key;

transmitting to the wireless local area network the second network to user device certificate, wherein the wireless local area network is able to derive the user public key using a broker public key received from the broker entity;

receiving, from the wireless local area network, a session key encrypted using the user public key;

decrypting the session key with a user private key; and

communicating with the wireless local area network using the session key.

PAGE 4/9 * RCVD AT 4/8/2008 8:20:38 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:609 734 6888 * DURATION (mm-ss):01-46

11. (original) The method of claim 10, wherein the second network to user certificate further includes a user subscription level that indicates whether a user has a subscription for an interworking service.

12. (original) The method of claim 10, wherein the second network to user certificate further includes an expiration time of the second network to user certificate, and the transmitting step is performed if the expiration time has not expired.

13. (original) The method of claim 10, wherein the receiving step comprises receiving a wireless local area network to user certificate signed with the broker private key and including the session key, and further comprising the steps of receiving the broker public key, and authenticating the wireless local area network to user certificate using the broker public key and deriving the session key.

14. (original) A broker based system for authenticating users in networks having interworking relationships, comprising:

a wireless local area network having an interworking function;

a second network; and

a broker capable of communicating with the wireless local area network and the second network, the broker having means for transmitting a broker public key to the wireless local area network, and means for transmitting a broker to second network certificate, which is signed with a broker private key and includes a second network public key, to the second network,

the second network including means for transmitting, to a user device, a second network to user certificate signed with a second network private key and includes the broker to second network certificate and the user public key,

the wireless local area network including means for authenticating the broker to second network certificate and deriving the second network public key, means for

PAGE 5/9 * RCVD AT 4/8/2008 8:20:38 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:609 734 6888 * DURATION (mm-ss):01-46

authenticating the second network to user certificate and deriving the user public key, and means for generating a session key and encrypting the session key with the user public key.

15. (currently amended) The ~~method~~ system of claim 14, wherein the wireless local area network further includes means for transmitting a wireless local area network to user certificate signed with a wireless local area network private key and includes the encrypted session key.

16. (new) A mobile device comprising:

means for receiving from a second network a second network to user certificate that includes a broker to second network certificate and a key;

means for transmitting said second network to user certificate to a first network;

means for receiving a session key generated by said first network; and

means for communicating with said first network using said session key.

17. (new) The mobile device according to claim 16, wherein said first network is a wireless local area network having an interworking function.

18. (new) The mobile device according to claim 16, wherein said second network is a cellular network.

PAGE 6/9 * RCVD AT 4/8/2008 8:20:38 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:609 734 6888 * DURATION (mm-ss):01-46